

On the Growth of Subalgebras in Lie p -Algebras

David Riley¹

*Department of Mathematics, Middlesex College, The University of Western Ontario,
London, Ontario N6A 5B7, Canada*

and

Vladimir Tasić¹

*Department of Mathematics and Statistics, University of New Brunswick, Fredericton,
New Brunswick E3B 5A3, Canada*

Communicated by A. Lubotzky

Received January 24, 2000

Let L be a finitely generated Lie p -algebra over a finite field F . Then the number, $a_n(L)$, of p -subalgebras of finite codimension n in L is finite. We say that L has PSG (polynomial p -subalgebras growth) if the growth of $a_n(L)$ is bounded above by some polynomial in $|F|^n$. We show that if L has PSG then the lower central series of L stabilises after a finite number of steps. On the other hand, if L is nilpotent then L has PSG. We deduce the following group-theoretic result. Let G be a group and let $G_{\hat{p}}$ denote a pro- p completion of G . Then the associated Lie p -algebra $\mathcal{L}_p(G)$ of G has PSG if and only if $G_{\hat{p}}$ is a p -adic analytic Lie group. © 2001 Academic Press

1. INTRODUCTION

The Lie algebras studied in this paper are restricted, which is to say, they possess a unary p -map, where $p > 0$ denotes the characteristic of the base field, with properties modeled on exponentiation by p in an associative algebra. Restricted Lie algebras are also called Lie p -algebras. The reader

¹The authors are supported by NSERC of Canada.

is referred to the monographs [J] and [SF] for basic background information. We shall work mainly within the category of restricted Lie algebras: the term p -subalgebra refers to a subalgebra that is also closed under the p -map, and so forth.

Given a restricted Lie algebra L , we assign to each integer $n \geq 0$ the cardinality $a_n(L)$ of the set of p -subalgebras H in L with $\dim(L/H) = n$.

THEOREM A. *If L is a finitely generated restricted Lie algebra over a finite field F then each of the cardinal numbers $a_n(L)$ is finite.*

One might suspect that Theorem A holds more generally. However, since any two-dimensional vector space over an infinite field possesses infinitely many subspaces of codimension 1, the assumption that F is finite is clearly necessary. As yet, we have been unable to decide whether or not the analogue of Theorem A holds for all modular Lie algebras. More generally, let us mention what we believe is an open problem: *Does every finitely generated Lie ring contain only a finite number of subrings of a given finite index?* It is known that the analogous problem for groups has a positive solution. Perhaps less well-known, but still true, is the corresponding fact for associative rings (see Remark 2.7).

Henceforth, F will denote a fixed field of characteristic p and finite cardinality q . All of our vector spaces will have the base field F .

We intend to study the structure of a finitely generated restricted Lie algebra L in terms of the growth of the integral sequence $a_n(L)$. Recall that if H is a subspace of L such that $\dim(L/H) = n$ then the additive index of H in L is $|L/H| = q^n$. It turns out that the additive index is a more natural choice of parameter than the codimension. We shall say that the sequence $a_n(L)$ grows polynomially if there exists a positive integer s such that

$$a_n(L) \leq (q^n)^s$$

for all n or, equivalently, if there exists a positive integer t such that

$$\sigma_n(L) \leq (q^n)^t$$

where

$$\sigma_n(L) := \sum_{i=0}^n a_i(L).$$

Clearly $\sigma_n(L)$ is the number of p -subalgebras of L of codimension at most n . In the case when $a_n(L)$ grows polynomially, we say that L has polynomial p -subalgebra growth, or L has PSG, for short. The degree of the growth of L is defined as

$$\alpha(L) = \limsup_{n \rightarrow \infty} \frac{\log_q \sigma_n(L)}{n}.$$

Let $d(L)$ denote the minimal cardinality of a set of generators required to generate an arbitrary restricted Lie algebra L . The p -subalgebra rank, $\text{rk}(L)$, of L is defined to be the supremum of the set of numbers $d(H)$, where H runs through all finitely generated p -subalgebras H in L . Because there will be no ambiguity in the following, we shall refer to $\text{rk}(L)$ merely as the rank of L .

Our main results are as follows.

THEOREM B. *Let L be a finitely generated restricted Lie algebra over a finite field. If L has PSG then the lower central series of L stabilises after a finite number of steps determined by the degree of the growth of L .*

Theorem B provides us with the most interesting implication in the following characterisation.

THEOREM C. *Let L be a finitely generated restricted Lie algebra over a finite field. If L is residually nilpotent then the following conditions are equivalent:*

1. L has PSG.
2. L is of finite rank.
3. L is centre-by-(finite-dimensional).
4. L is nilpotent.

In order to study the property PSG more generally, it is sensible to focus on the class of residually finite-dimensional restricted Lie algebras. Under this natural stipulation, it seems conceivable that the first three conditions of Theorem C will remain equivalent.

We note that restricted Lie algebras of finite rank are studied more generally in [R] and [RS], while ordinary Lie algebras of finite rank are examined in [ER].

Recently, much attention has been devoted to the study of groups and profinite groups with polynomial subgroup growth, which provided the initial motivation for this present study. See, in particular [LM, LMS, MS, and SS]. Similar notions in the category of modules over commutative rings are investigated in [S].

To each group G it is possible to associate a restricted Lie algebra $\mathcal{L}_p(G)$ over the field of p -elements. The details of this construction are outlined in Section 7. As a final application of our theorem, we shall deduce the following result.

THEOREM D. *Let G be a group and let $G_{\hat{p}}$ be a pro- p completion of G . Then $\mathcal{L}_p(G)$ has polynomial p -subalgebra growth if and only if $G_{\hat{p}}$ has polynomial subgroup growth.*

It was proved in [LM] that a pro- p group has polynomial subgroup growth precisely when it is p -adic analytic.

Finally, we remark that our techniques will yield explicit bounds in each of the results above.

2. PROOF OF THEOREM A

Let $h(x, y)$ denote the function defined recursively by

$$h(x, 0) = x,$$

$$h(x, y + 1) = h(x, y)(h(x, y) + 1).$$

A close examination of the proof of Lemma 10 in [K] yields the following quantitative version.

LEMMA 2.1. *Let L be a restricted Lie algebra over an arbitrary field of characteristic p , and let H be a p -subalgebra of codimension n in L . Then there exists a p -ideal I in L contained in H such that $\dim(L/I) \leq h(n, n^p)$.*

Consequently, we may define the core of the p -subalgebra H in L to be the unique maximal p -ideal $\text{core}(H)$ in L contained in H . So, $\dim(L/H) = n$ implies $\dim(L/\text{core}(H)) \leq h(n, n^p)$.

Interestingly, there is no analogue of this notion for Lie algebras of characteristic zero as the following Witt algebra demonstrates.

EXAMPLE 2.2. Let L be the Lie algebra over any field of characteristic zero presented by generators $\{e_n \mid n \geq -1\}$ and relations $[e_i, e_j] = (i - j)e_{i+j}$. Then the subalgebra H spanned by $\{e_0, e_1, \dots\}$ has codimension 1 in L , while it does not contain any finite-codimensional ideals of L since L is simple.

Let $b_n(L)$ denote the cardinality of the set of p -ideals I in L such that $\dim(L/I) = n$.

LEMMA 2.3. *Let L be a finitely generated restricted Lie algebra over a finite field F . Then each $b_n(L)$ is finite. Moreover, if L is d -generated and $|F| = q$ then $b_n(L) \leq t_n q^{nd}$, where t_n is the number of isomorphism types of restricted Lie algebras of dimension n over F .*

Proof. Indeed, suppose that I is a p -ideal in L such that $\dim(L/I) = n$, and let M_1, \dots, M_{t_n} be representatives of the isomorphism types of restricted Lie algebras of dimension n . Then there is an isomorphism $\phi: L/I \rightarrow M_1$, say. Consider the natural map $\theta: L \rightarrow L/I$. Then $\ker(\phi \circ \theta) = \ker \theta = I$. Hence, $I = \ker \psi$ for some homomorphism $\psi: L \rightarrow M_1$. Because $|M_1| = q^n$ and L is d -generated, there are at

most q^{nd} -many homomorphisms $\psi : L \rightarrow M_1$. Similarly, there are at most q^{nd} -many homomorphisms $\psi : L \rightarrow M_i (1 \leq i \leq t_n)$. In consequence, there are at most $t_n q^{nd}$ -many p -ideals I in L with $\dim(L/I) = n$. ■

The following result is an exercise in linear algebra.

LEMMA 2.4. *Let V be an n -dimensional vector space over a finite field F , $|F| = q$. Let $c(n, r)$ denote the number of r -dimensional subspaces of V . Then*

$$c(n, r) = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-r+1} - 1)}{(q^r - 1)(q^{r-1} - 1) \cdots (q - 1)}.$$

Moreover, the number of subspaces of codimension r equals $c(n, n - r) = c(n, r)$.

We shall require some weak estimates of $c(n, r)$ in the following. Expansion proves the inequalities

$$(q^i - 1)q^{j-i} < q^j - 1 \leq (q^i - 1)(1 + q + \cdots + q^{j-i})$$

for all $1 \leq i < j$. It follows that

$$q^{(n-r)r} < c(n, r) \leq (1 + q + \cdots + q^{n-r})^r$$

for all $1 \leq r < n$.

The proof of the next lemma is straightforward and thus omitted.

LEMMA 2.5. *Let I be a p -ideal in a restricted Lie algebra L . Then $a_n(L/I) \leq a_n(L)$ for each n . Thus $\sigma_n(L/I) \leq \sigma_n(L)$ for each n .*

THEOREM 2.6. *Let L be a finitely generated restricted Lie algebra over a finite field F . Then each $a_n(L)$ is finite. Furthermore, if L is d -generated and $|F| = q$, we have $a_n(L) \leq c(h(n, n^q)t_{h(n, n^q)}q^{h(n, n^q)d}, n)$, a function depending only on d, q , and n .*

Proof. Put $m = h(n, n^p)$, where h is the recursive function introduced at the beginning of this section. By Lemma 2.3, $b_m(L) \leq t_m q^{md}$. Let J be the intersection of all p -ideals in L of index at most m . Then $\dim(L/J)$ is bounded by $mb_m(L) \leq mt_m q^{md}$. By Lemma 2.5 this yields

$$a_n(L) = a_n(L/J) \leq c(\dim(L/J), n) \leq c\left(h(n, n^p)t_{h(n, n^p)}q^{h(n, n^p)d}, n\right).$$

Crudely estimating $p \leq q$ now gives us the result. ■

This completes the proof of Theorem A.

REMARK 2.7 Let R be a finitely generated (associative) ring. Then the number of subrings of a given additive index in R is finite.

Indeed, it can be deduced from arguments of Hirano [H] that if S is an additive subgroup of R of finite index n , then S contains an ideal of R that is of finite index bounded above by a function of n only. The claim now follows as in the proof of Theorem A.

3. MORE NOTATION

In order to proceed with the remainder of the proof, we need several definitions. The reader is referred to [RS] and [RSh] for further details.

For an arbitrary restricted Lie algebra L , we let L_n denote the n th member of the lower central series of L , that is, the p -subalgebra of L generated by the elements of the form $[x_1, \dots, x_n]$, where $x_j \in L$. Further, L^{p^i} is defined as the p -subalgebra generated by the elements x^{p^i} , where $x \in L$. A restricted Lie algebra L is said to be nilpotent if $L_m = 0$ for some integer m ; the minimal number c such that $L_{c+1} = 0$ is the class, $\text{cl}(L)$, of L . We say that the restricted Lie algebra L is p -nilpotent if there is an integer k such that $L^{p^k} = 0$.

The n th dimension subalgebra of L is defined as

$$D_n(L) = \sum_{ip^j \geq n} L_i^{p^j}.$$

These p -subalgebras arise naturally in connection with the restricted universal enveloping algebra of L (see [RSh]). Because every restricted Lie algebra satisfies the axiom

$$[x, y^p] = [x, \underbrace{y, \dots, y}_p],$$

it follows that $D_n(L)$ is a descending series of p -ideals such that, for all positive integers m and n , $[D_n(L), D_m(L)] \subseteq L_{m+n}$ and $D_m(L)^p \subseteq D_{mp}(L)$.

Let \mathcal{F}_p denote the class of those finite-dimensional restricted Lie algebras whose p -map is nilpotent. From Engel's theorem it follows that the algebras in this class are nilpotent.

According to a result of Lincoln and Tower [LT], if L lies in the class \mathcal{F}_p then $D_2(L)$ coincides with the Frattini p -subalgebra of L , that is, the intersection of all maximal p -subalgebras in L . It follows that $d(L) = \dim(L/D_2(L))$.

Finally, within the class \mathcal{F}_p , we define the algebra L to be powerful if $L' \subseteq D_3(L)$, where L' is the derived subalgebra of L . This is equivalent to the statements that $L' \subseteq L^p$ when p is odd and $L' \subseteq L^4$ if $p = 2$. In fact, we may replace L^p with merely the set $L^{\{p\}}$ of p -powers in L when p is odd and with the set of 4-powers $L^{\{4\}}$ when $p = 2$ (see Proposition 5.2 in [RS]).

4. NILPOTENT RESTRICTED LIE ALGEBRAS

The principal aim of this section is to prove that every finitely generated nilpotent restricted Lie algebra over a finite field has PSG.

LEMMA 4.1. *If L is an m -generated abelian restricted Lie algebra over the field $F = \text{GF}(p)$ of p elements then $\sigma_n(L) \leq (p^n)^{m(m+1)}$.*

Proof. By Lemma 2.5, it suffices to prove this in the case when L is a free abelian restricted Lie algebra, so we let L have free generators x_1, \dots, x_m . Let ∂ denote the p -map. By our choice of base field, ∂ is an endomorphism of the vector space L . Therefore, L has a natural structure as a module over $D = F[\partial]$. Note that the freeness of L implies $D \cong F[x]$, so that L is a faithful module over a Euclidean domain. It is clear that L is a free D -module of rank m . Also, any p -subalgebra of L is a D -submodule of L and the converse.

Let H be a p -subalgebra of codimension n in L . Since L/H is finite-dimensional, there are polynomials $d_1, \dots, d_m \in D$, each of degree at most n , such that $d_i x_i \in H$. Define H_0 to be the submodule of H generated by $\{d_1 x_1, \dots, d_m x_m\}$. Note that $L/H_0 \cong D/d_1 D \oplus \dots \oplus D/d_m D$. Hence L/H_0 is a direct sum of m cyclic D -modules of dimension at most n and thus $\dim_F(L/H_0) \leq nm$. Because H_0 is completely determined by the m -tuple (d_1, \dots, d_m) , there are at most p^{nm} possibilities for H_0 .

Note that H is uniquely determined by H_0 and a submodule K/H_0 of L/H_0 . We have to estimate the number of such submodules K/H_0 . Since L/H_0 is a direct sum of m cyclic modules, it follows that K/H_0 can be generated by m elements. Each of these generators is a linear combination over D of the elements $x_i + H_0$ of L/H_0 . Thus every m -tuple of D -module generators for K/H_0 is uniquely determined by a D -endomorphism of $L/H_0 \cong D/d_1 D \oplus \dots \oplus D/d_m D$. There are at most p^{nm^2} such endomorphisms, which gives an upper bound on the number of appropriate submodules K/H_0 .

The number of submodules H is bounded by the product of the number of submodules H_0 and the number of submodules K/H_0 . Consequently, we have $\sigma_n(L) \leq p^{nm^2 + nm}$, as required. ■

LEMMA 4.2. *Let L be an m -generated abelian restricted Lie algebra over a finite field F with q elements. Then $\sigma_n(L) \leq (q^n)^{mq(mq+1)}$.*

Proof. Suppose L is generated by x_1, \dots, x_m as an abelian restricted Lie algebra over F . Because the field F is perfect, it is easy to see that L can be considered as an abelian restricted Lie algebra over $\text{GF}(p)$, with mq generators $y_{\theta,i} = \theta x_i$ ($\theta \in F$, $1 \leq i \leq m$). Applying the preceding lemma, we obtain that

$$\sigma_{n, \text{GF}(p)}(L) \leq p^{n(m^2 q^2 + mq)}$$

for each n . Now let H be a p -subalgebra of L such that $\dim_F(L/H) = n$. Then $\dim_{\text{GF}(p)}(L/H) = kn$, where $k = \dim_{\text{GF}(p)} F$. Hence

$$\sigma_{n,F}(L) \leq \sigma_{kn,\text{GF}(p)}(L) \leq p^{kn(m^2q^2+mq)} = q^{n(m^2q^2+mq)},$$

as required. ■

LEMMA 4.3. *Let L be a restricted Lie algebra over a q -element field. If H is a p -subalgebra of finite codimension k then $\sigma_n(L) \leq [(n+1)q^n]^k \sigma_n(H)$ for every n . It follows that $\alpha(L) \leq \alpha(H) + k$.*

Proof. Let S be any p -subalgebra of L with codimension at most n . Then $H/(S \cap H) \cong (H + S)/S$, as vector spaces, so that $J = S \cap H$ is a p -subalgebra of codimension at most n in H . Similarly, $S/(H \cap S) \cong (S + H)/H$ as vector spaces, so that $\dim(S/J) \leq \dim(L/H) = k$. Hence, for every p -subalgebra S of codimension at most n in L there exists a p -subalgebra K of H with $\dim(H/K) \leq n$ and $\dim(S/K) \leq k$. By definition, there are at most $\sigma_n(H)$ possibilities for K . Fixing K , we may write $\dim(S/K) = i$ where $0 \leq i \leq k$; in other words, $\dim(L/K) = n + i$. Again by definition, the number of subspaces of L/K of dimension i is $c(n + i, i)$. By Lemma 2.4 and the subsequent comments,

$$c(n + i, i) = c(n + i, n) \leq c(n + k, n) = c(n + k, k) \leq [(n + 1)q^n]^k.$$

Combining yields

$$\sigma_n(L) \leq [(n + 1)q^n]^k \sigma_n(H),$$

as required. ■

We shall require the following theorem due to Witt (see [B] for a proof).

THEOREM 4.4. *Every p -subalgebra of finite codimension k in a d -generated restricted Lie algebra (over an arbitrary field of characteristic $p > 0$) can be generated by $p^k(d - 1) + 1$ many elements.*

COROLLARY 4.5. *Let L be a d -generated restricted Lie algebra over a field with q elements. If the centre of L has finite codimension k in L then L has PSG with $\alpha(L) \leq mq(mq + 1) + k$, where $m = p^k(d - 1) + 1$.*

Proof. By Witt's theorem above, the centre $H = \zeta(L)$ is an m -generated abelian p -subalgebra of L . According to Lemma 4.2, this means $\sigma_n(H) \leq (q^n)^{mq(mq+1)}$. Applying Lemma 4.3 now yields the result. ■

Given a real number x , let $\lceil x \rceil$ denote the least integer greater than or equal to x .

COROLLARY 4.6. *Let L be a d -generated restricted Lie algebra that is nilpotent of class c . Then L has PSG with $\alpha(L) \leq mq(mq + 1) + k$, where $m = p^k(d - 1) + 1$, $k = \sum_{i=1}^s d^i \lceil \log_p(s/i) \rceil$, and $s = \lceil (c + 1)/2 \rceil$. In particular, $\alpha(L)$ is bounded above by a function of d , c , and q only.*

Proof. Note that $D_s(L)$ is abelian since $[D_s(L), D_s(L)] \subseteq L_{c+1} = 0$. The integer k is a crude upper bound on $\dim(L/D_s(L))$: see the proof of Proposition 6.9 in [RS] for details. The result now follows as in the previous corollary, this time with $H = D_s(L)$. ■

This establishes the implication (4) \Rightarrow (1) of Theorem C, while Corollary 4.5 establishes the implication (3) \Rightarrow (1) of the same theorem. A slight modification of the proof of Corollary 4.6 (with $D_c(L)$ in place of $D_s(L)$) also shows (4) \Rightarrow (3).

5. LIE p -ALGEBRAS OF FINITE RANK

Let \mathcal{C} denote the class obtained from all soluble restricted Lie algebras (over an arbitrary field of positive characteristic) by closing under the operations L and R , where, for any restricted Lie-theoretical class \mathcal{X} , $L\mathcal{X}$ denotes the class of all restricted Lie algebras locally in \mathcal{X} and $R\mathcal{X}$ denotes the class of all restricted Lie algebras residually in \mathcal{X} .

The following result follows immediately from Theorems A and B in [R]. A stronger, quantitative version also holds.

THEOREM 5.1. *Let L denote a restricted Lie algebra over an arbitrary field of positive characteristic.*

1. *If L is of finite rank and \mathcal{C} -by-(finite-dimensional) then L is centre-by-(finite-dimensional).*
2. *If L is finitely generated and centre-by-(finite-dimensional) then L is of finite rank.*

The equivalence of conditions (2) and (3) in Theorem C is clearly a special case of Theorem 5.1. Since we have already seen (4) \Rightarrow (3) \Rightarrow (1), it suffices to prove Theorem B in order to complete the proof of Theorem C.

6. PROOF OF THEOREM B

We now examine restricted Lie algebras with PSG of a given degree. This is accomplished through a careful study of this property in the class \mathcal{F}_p and the subclass of powerful restricted Lie algebras. Our line of attack is similar to that employed by Lubotzky and Mann in their study of pro- p groups with polynomial subgroup growth (see [DDMS] and [LM]).

LEMMA 6.1. *Let $L \in \mathcal{F}_p$ be such that $a_1(L) \leq q^s$. Then $d = d(L) \leq s$.*

Proof. Let $\bar{L} = L/D_2(L)$. Then, by Lemma 2.5, $a_1(\bar{L}) \leq a_1(L) \leq q^s$. In \bar{L} every subspace is a p -subalgebra. It follows that

$$q^{d-1} < c(d, 1) = c(\dim(\bar{L}), 1) = a_1(\bar{L}) \leq q^s,$$

as required. ■

Let s, t be positive integers. Define $\lambda(t) = \lceil \log_2 t \rceil$. Next, set $\tau(s)$ to be the maximal positive integer t such that

$$\frac{t^2 - 1}{4} \leq \left(\left\lceil \frac{t}{2} \right\rceil + (t-1)\lambda(t) \right) s.$$

LEMMA 6.2. *Let $L \in \mathcal{F}_p$. Choose r to be the maximal integer such that $r = d(I)$ for some p -ideal I in L . Let M be maximal amongst the set of p -ideals I in L with $d(I) = r$. Set C to be the centraliser of $M/D_2(M)$ in L . Then $C = M$ and $\dim(L/M) \leq (r-1)\lambda(r)$.*

Proof. It is easily verified that C is a p -ideal in L containing M . Suppose that C/M is nontrivial. Because L/M lies in the (nilpotent) class \mathcal{F}_p , C/M possesses a nonzero element $x + M$ of exponent p that is central in L/M . Let $I = M + Fx$. Then I is a p -ideal in L properly containing M . But certainly $D_2(I) = D_2(M) = 0$, so that

$$d(I) = \dim(I/D_2(I)) > \dim(M/D_2(M)) = d(M) = r,$$

contrary to our choice of r . Consequently, $C = M$ as claimed.

The first claim implies that L/M acts faithfully on the r -dimensional vector space $M/D_2(M)$. Therefore $D_r(L/M) = 0$. See 6.3 in [RS] for details. Next, by our choice of M and r , every p -ideal of L/M is $(r-1)$ -generated. It follows that each of the elementary p -abelian factors $D_{2^i}(L/M)/D_{2^{i+1}}(L/M)$ is at most $(r-1)$ -dimensional. This proves the second claim. ■

LEMMA 6.3. *If L lies in the class \mathcal{F}_p and $\sigma_n(L) \leq q^{ns}$, for all $n \geq 0$, then $d(I) \leq \tau(s)$ for each p -ideal I in L .*

Proof. Suppose otherwise and choose r to be the maximal integer such that $r = d(I)$ for some p -ideal I in L . Let M be maximal amongst the set of p -ideals I in L with $d(I) = r$. Then $r > \tau(s)$, by assumption.

Now, by Lemma 6.2, we know $\dim(L/M) \leq (r-1)\lambda(r)$. On the other hand, $\dim(M/D_2(M)) = r$, so that $M/D_2(M)$ contains at least $q^{(r^2-1)/4}$ -many p -subalgebras of codimension $\lceil r/2 \rceil$ since

$$q^{(r^2-1)/4} \leq q^{(r-\lceil r/2 \rceil)\lceil r/2 \rceil} \leq c(r, \lceil r/2 \rceil).$$

Thus, $q^{(r^2-1)/4} \leq a_{\lceil r/2 \rceil}(M)$. This yields

$$q^{(r^2-1)/4} \leq \sigma_{(\lceil r/2 \rceil + (r-1)\lambda(r))}(L) \leq q^{(\lceil r/2 \rceil + (r-1)\lambda(r))s},$$

contrary to the definition of $\tau(s)$. ■

The next three lemmas correspond to Proposition 6.4, Theorem 6.2, and Lemma 6.7, respectively, in [RS].

LEMMA 6.4. *Let $L \in \mathcal{F}_p$. Suppose that $d(D_r(L)) \leq r$ for some integer r . Then $D_r(L)$ is powerful if p is odd, while $D_r(L)^2$ is powerful if $p = 2$.*

LEMMA 6.5. *If $L \in \mathcal{F}_p$ is powerful then $\text{rk}(L) = d(L)$.*

LEMMA 6.6. *Let $L \in \mathcal{F}_p$. If I is a p -ideal in L then $\text{rk}(L) \leq \text{rk}(I) + \text{rk}(L/I)$.*

Let us introduce a convenient notation: Set $\epsilon = 0$ if p is odd and $\epsilon = 1$ if $p = 2$.

PROPOSITION 6.7. *Suppose that L lies in the class \mathcal{F}_p and $\sigma_n(L) \leq q^{ns}$ for all n . Put $r = \tau(s)$. Then the following statements hold:*

1. $\dim(L/\zeta(L)) \leq s + r(2\epsilon + \lambda(r))$.
2. $\text{cl}(L) \leq s + r(2\epsilon + \lambda(r))$.
3. $\text{rk}(L) \leq s + r(\epsilon + \lambda(r))$.

Proof. From Lemma 6.1, we have $\dim(L/D_2(L)) = d(L) \leq s$. By Lemma 6.3, $d(I) \leq r$ for every p -ideal I in L , so that $\dim(I/D_2(I)) = d(I) \leq r$.

Consider first the case that p is odd and put $I = D_r(L)$. Then $\dim(L/I) \leq s + r(\lambda(r) - 1)$ since for each $i \geq 1$ we have $d(D_{2^i}(L)) \leq r$. Applying Lemma 6.4 yields that I is powerful. That is, $I_2 \subseteq D_2(I) = I^{\{p\}}$, and so

$$I_3 = [I, I_2] \subseteq [I, I^{\{p\}}] \subseteq [I, {}_p I] = I_{p+1}.$$

Because

$$I_3 \subseteq [L, D_2(I)] = [L, I^{\{p\}}] \subseteq [L, {}_p I] \subseteq I_p,$$

and since $p \geq 3$, it follows that $D_2(I)$ is central in L . Consequently,

$$\dim(L/\zeta(L)) \leq \dim(L/I) \leq \dim(I/D_2(I)) + \dim(L/I) \leq s + r\lambda(r),$$

proving Part 1. Part 2 follows easily from Part 1. To see why Part 3 holds, note that Lemmas 6.5 and 6.6 imply

$$\text{rk}(L) \leq \text{rk}(I) + \text{rk}(L/I) \leq d(I) + \dim(L/I) \leq s + r\lambda(r).$$

In the case $p = 2$, we set $I = D_r(L)^2$. In fact, $I = D_2(D_r(L))$ because $D_r(L)/I$ is abelian. Observe that if J is a 2-ideal in L then so is $D_2(J)$. Since $\dim(J/D_2(J)) = d(J) \leq r$, it follows by induction that $\dim(L/I) \leq s + r\lambda(r)$. By Lemma 6.4, I is powerful, so that $I_2 \subseteq D_3(I) = I^{\{4\}}$. Thus

$$I_3 = [I, I_2] \subseteq [L, D_3(I)] = [L, I^{\{4\}}] \subseteq [L, {}_4I] \subseteq I_4,$$

implying that $D_3(I)$ is central in L . Since $D_2(D_2(I)) \subseteq D_4(I) \subseteq D_3(I)$, it follows that $\dim(I/D_3(I)) \leq 2r$. Thus, $\dim(L/\zeta(L)) \leq s + r(2 + \lambda(r))$, proving Parts 1 and 2. To see why Part 3 holds, note that this time Lemmas 6.5 and 6.6 imply

$$\mathrm{rk}(L) \leq \mathrm{rk}(I) + \mathrm{rk}(L/I) \leq d(I) + \dim(L/I) \leq r + (s + r\lambda(r)).$$

■

THEOREM 6.8. *Let L be a finitely generated residually nilpotent restricted Lie algebra over a field F with q elements. If L has PSG then L is nilpotent. Moreover, if s is the minimal positive integer such that $\sigma_n(L) \leq q^{ns}$ for every n and $r = \tau(s)$ then the following statements hold:*

1. $\dim(L/\zeta_2(L)) \leq s + r(2\epsilon + \lambda(r))$.
2. $\mathrm{cl}(L) \leq s + r(2\epsilon + \lambda(r)) + 1$.

Proof. We prove Part 2 first. Consider $N = L/L_m$ where m is a large positive integer. Put $\bar{N} = N/\zeta(N)$. Two applications of Lemma 2.5 show that $\sigma_n(\bar{N}) \leq q^{ns}$ for every n . Since N is finitely generated and nilpotent, \bar{N} lies in the class \mathcal{F}_p . Part 2 of Proposition 6.7 now yields $\mathrm{cl}(\bar{N}) \leq s + r(2\epsilon + \lambda(r))$, so that $\mathrm{cl}(N) \leq s + r(2\epsilon + \lambda(r)) + 1$. Because L is residually nilpotent, Part 2 of the theorem follows.

Now L is finitely generated and nilpotent, so that $\bar{L} = L/\zeta(L)$ lies in the class \mathcal{F}_p . Applying Part 1 of Proposition 6.7 to \bar{L} now yields Part 1 of the theorem since $\dim(L/\zeta_2(L)) = \dim(\bar{L}/\zeta(\bar{L}))$. ■

We have the following immediate corollary.

COROLLARY 6.9. *Suppose L is any finitely generated restricted Lie algebra over F with PSG. Choose the minimal positive integer s such that $\sigma_n(L) \leq q^{ns}$ for every n and put $r = \tau(s)$. Then $L_{s+r(2\epsilon+\lambda(r))+2} = L_{s+r(2\epsilon+\lambda(r))+3}$.*

This concludes our quantitative proof of Theorem B. It is easy to check that given any real number $\eta > 0$ we have

$$\lim_{s \rightarrow \infty} \frac{\tau(s)}{s(\log_2 s)^{1+\eta}} = 0.$$

It follows now from the corollary that there exists an integer s_0 such that, given $s \geq s_0$, we have $L_t = L_{t+1}$ for all $t \geq s(\log_2 s)^2$, regardless of the choice of L .

7. PROOF OF THEOREM D

The restricted Lie GF(p)-algebra associated to a group G is defined by

$$\mathcal{L}_p(G) = \bigoplus_{m \geq 1} D_m(G)/D_{m+1}(G).$$

Here $D_m(G)$ denotes the m th dimension subgroup of G , given by $D_m(G) = G \cap (1 + \Delta(G)^m)$, where $\Delta(G)$ denotes the augmentation ideal of the group algebra of G over the field GF(p). Commutation and exponentiation by p in G induce the restricted Lie structure on $\mathcal{L}_p(G)$.

In order to prove Theorem D we shall require several known results about pro- p groups for which [DDMS, L, and LM] are sufficient sources.

Let Γ be a pro- p group. Lazard proved that Γ is a p -adic analytic Lie group precisely when $\mathcal{L}_p(\Gamma)$ is finitely generated and nilpotent. On the other hand, it follows from a result of Lubotzky and Mann that Γ is p -adic analytic if and only if it has polynomial subgroup growth.

Now, to prove Theorem D, let G be a group such that some pro- p completion Γ of G has polynomial subgroup growth. It follows that Γ is (topologically) finitely generated, and hence uniquely determined by a theorem of Serre. Thus, we may as well complete G with respect to its dimension subgroups, so that clearly $\mathcal{L}_p(\Gamma) \cong \mathcal{L}_p(G)$. According to the preceding paragraph, $\mathcal{L}_p(G)$ is therefore finitely generated and nilpotent, and so has polynomial p -subalgebra growth by Theorem C.

Conversely, suppose $\mathcal{L}_p(G)$ has polynomial p -subalgebra growth. Then since $\mathcal{L}_p(G)$ is residually nilpotent, $\mathcal{L}_p(G)$ is in fact nilpotent by Theorem C. Also, by Lemma 6.1, it follows that $\mathcal{L}_p(G)$ is finitely generated. Hence $G/D_2(G)$ is finite, which implies that the pro- p completion Γ of G is uniquely determined and finitely generated. Consequently, $\mathcal{L}_p(\Gamma) \cong \mathcal{L}_p(G)$ and Γ has polynomial subgroup growth as outlined above.

In fact, with slightly more work, a quantitative relationship between the growth of G and the growth $\mathcal{L}_p(G)$ can be found by combining our Proposition 6.7 with the proof of Theorem 3.19 in [DDMS] via Theorem 8.5 in [RS]. These bounds seem fairly reasonable, but certainly are not sharp.

It would be interesting to study the relationship between the growth of G and the growth of $\mathcal{L}_p(G)$ in the case when G is not p -adic analytic.

COROLLARY 7.1. *Let G be a group. Then $\mathcal{L}_p(G)$ has PSG if and only if its (unique) pro- p completion $G_{\hat{p}}$ is p -adic analytic.*

REFERENCES

- [B] Y. Bahturin, "Identical Relations in Lie Algebras," VNU Science Press, Utrecht, 1987.
- [DDMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, "Analytic pro- p Groups," Cambridge Univ. Press, Cambridge, UK, 1991.
- [ER] M. J. Evans and D. M. Riley, Lie algebras of finite subalgebra rank, *Arch. Math.* **69** (1997), 185–191.
- [H] Y. Hirano, On extensions of rings with finite additive index, *Math. J. Okayama Univ.* **32** (1990), 93–95.
- [J] N. Jacobson, "Basic Algebra I," W. H. Freeman, San Francisco, 1974.
- [K] G. P. Kukin, The equality problem and free products of Lie algebras and associative algebras, *Siber. Math. J.* **24**, No. 2 (1983), 221–231.
- [L] M. Lazard, Groupes analytiques p -adiques, *Publ. Math. Inst. Hautes Etudes Sci.* **26** (1965), 389–603.
- [LT] M. Lincoln and D. Towers, Frattini theory for restricted Lie algebras, *Arch. Math.* **45** (1985), 451–457.
- [LM] A. Lubotzky and A. Mann, Powerful p -groups, I & II, *J. Algebra* **105** (1987), 484–515.
- [LMS] A. Lubotzky, A. Mann, and D. Segal, Finitely generated groups of polynomial subgroup growth, *Israel J. Math.* **82**, Nos. 1–3 (1993), 363–371.
- [MS] A. Mann and D. Segal, Subgroup growth: Some current developments," *Infinite Groups 1994*, Ravello, pp. 179–197, de Gruyter, Berlin, 1996.
- [R] D. M. Riley, Lie p -algebras of finite p -subalgebra rank, *Arch. Math.*, to appear.
- [RS] D. M. Riley and J. F. Semple, Completion of restricted Lie algebras, *Israel J. Math.* **86** (1994), 277–299.
- [RSh] D. M. Riley and A. Shalev, Restricted Lie algebras and their envelopes, *Canad. J. Math.* **47**, No. 1 (1995), 146–164.
- [S] D. Segal, On the growth of ideals and submodules, *J. London Math. Soc. (2)* **56**, No. 2 (1997), 245–263.
- [SS] D. Segal and A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math. Soc. (2)* **55** (1997), 320–334.
- [SF] H. Strade and R. Farnsteiner, "Modular Lie Algebras and Their Representations," Dekker, New York, 1998.